UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	)	
	)	
Dropbox.com account registered to the email address: talentedtongue14@yahoo.com	)	Magistrate No. **[UNDER SEAL]** 16-0182M

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Molly Rock, being duly sworn, do hereby depose and state:

1. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the HSI Pittsburgh, Pennsylvania office. I have been so employed since August, 2010. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a)(2), and 2252(a)(4)(B). I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

2. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records. This affidavit is submitted in support of an application for a search warrant authorizing the search and seizure of the Dropbox.com (hereinafter referred to as Dropbox) account registered to the email address talentedtongue14@yahoo.com.

3. The purpose of this application is to seize evidence, contraband, fruits, and other items related to violations of 18 U.S.C. §§ 2252(a)(2), which make it a crime to receive and distribute child pornography in interstate commerce by computer, and violations of 18 U.S.C. §§ 2252(a)(4)(B), which make it a crime to possess or access with intent to view child pornography (collectively, the "Specified Federal Offenses").

4. Because this Affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to search the Dropbox.com account registered to the email address talentedtongue14@yahoo.com.

LEGAL AUTHORITY

5. Title 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contained materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

6. Title 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate of foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

DEFINITIONS

7. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their

computer system for their subscribers' use. This service by ISPs allows for both temporary and long term storage of electronic communications and many other types of electronic data and files. Typically, email that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that email to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service."

h. An "electronic communications service," as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

i. "Domain names" are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server

located at the United States Department of Justice, which is part of the United States government.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

DROPBOX, Inc.

8. Dropbox is a file hosting service operated by Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents), regardless of which computer is used to view it. Files placed in this folder are also accessible through website and mobile phone applications.

9. Dropbox users sign up for an account with a valid e-mail address. Dropbox provides users with a certain amount of free data storage, and if the user wants more storage, the user can pay for it. Users can access Dropbox from anywhere in the world using the Internet. For example, a user may take a photograph from a smartphone, upload that photo to Dropbox, and then erase the photo from the user's phone. The photograph now resides in the user's "cloud." The user can then access his/her Dropbox account from a desktop computer and download the photograph to that computer.

10. Another feature of Dropbox is sharing. A Dropbox user can share certain files he/she designates by sending a web link to another user(s). It then gives the additional user(s) access to those particular files.

11. Your Affiant knows that Dropbox maintains records on their users, such as basic subscriber information within the meaning of 18 U.S.C § 2703(c)(2). Furthermore, your Affiant knows that Dropbox keeps and maintains the stored content of user accounts, such as photographs, movies, documents and music within the meaning of the Stored Communication Act. Once the records are received, government investigators will review the records and copy those files that are specified in Attachment B.

BACKGROUND REGARDING CHILD PORNOGRAPHY AND COMPUTERS

12. Based on your Affiant's training, experience, and knowledge, your Affiant knows the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and mobile devices (e.g., smartphones, tablets) has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers and mobile devices serve four functions in connection with child pornography; production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs directly from a camera or mobile device to a computer storage system. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem, or via mobile devices. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer and Internet-capable mobile devices are preferred methods of distribution and receipt of child pornographic materials.

d. The advent of webcams has enabled child pornographers to broadcast live transmissions of sexual abuse of minors by connecting the webcam to the Internet. A webcam is a video camera that attaches to a computer or that is built into a laptop or desktop screen. The software included with webcams also permits an individual to capture and save live transmissions to the computer or peripheral storage devices. A webcam can be used in conjunction with an instant messaging service which permits real-time, direct, text-based communication between two or more people while permitting the individuals to view each other

real-time via the webcam. However, a webcam is not required in order to receive live transmissions of activity that is taking place in front of another user's webcam.

e. The ability of a computer or mobile device to store images in digital form makes these devices an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text, and CDs, DVDs, and flash drives can store hundreds of images and thousands of pages of text. The size of the electronic storage media (commonly referred to as the hard drive or thumb drive) used in home computers has grown tremendously within the last several years. Electronic storage devices with the capacity of 750 gigabytes are common, and electronic storage devices in excess of one terabyte (1,000 gigabytes) are now available for sale for low cost. These drives can store thousands of images at very high resolution. It is possible to use digital cameras and "video" cameras (designed primarily to record moving images), including those contained in mobile devices, to upload images to the Internet. Only through careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail generated by this activity.

f. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

g. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography in various formats, including services offered by Internet Portals such as Microsoft Live, Yahoo!, Google, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or electronic device such as a phone, tablet, or

other device with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer and/or mobile devices, in most cases.

h. As is the case with most digital technology, communications by way of computer and mobile device can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files, cache, or ISP client software, among others). In addition to electronic communications, a computer or mobile device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. For example, computers often indefinitely retain archived conversations from instant messaging programs as well as messaging logs and files shared over instant messaging.

BACKGROUND OF THE INVESTIGATION & PROBABLE CAUSE

13. In May 2014, special agents from HSI Los Angeles executed a federal search warrant authorizing the search of a target's residence for violations relating to the distribution, receipt, and possession of child pornography. During the execution of the search warrant, the target of the investigation was interviewed and consented to law enforcement taking over the target's online presence, which included several different email accounts that the target used to trade child pornography.

14. HSI Riverside Special Agent (SA) Jonathan Ruiz took control of the aforementioned target's email accounts and periodically logged into these accounts, noting that the accounts continued to receive individual and group emails containing child pornography. On or about August 7, 2015, SA Ruiz logged into one of the accounts and found that the user of the email account talentedtongue19@yahoo.com had recently sent two group emails, each containing an attached child pornography video. The emails from talentedtongue19@yahoo.com were sent to the target account, as well as approximately 90 other email recipients.

15. On August 27, 2015, SA Ruiz executed a federal search warrant on Yahoo! for the user account talentedtongue19@yahoo.com to search for evidence of the distribution, receipt, and possession of child pornography. During October 2015, Yahoo! provided SA Ruiz with information responsive to the aforementioned search warrant. SA Ruiz reviewed the information provided by Yahoo! and noted that the talentedtongue19@yahoo.com account contained numerous emails, both sent and received, that included attached images and/or videos depicting the sexual exploitation of minors, as well as discussions of the sexual abuse of children. In addition, SA Ruiz found emails sent by talentedtongue19@yahoo.com that contained hyperlinks to downloadable files, as well as solicitations to others offering to trade child pornography.

16. SA Ruiz subsequently obtained the hash values of the images and videos contained in the talentedtongue19@yahoo.com account and submitted the information to the National Center for Missing and Exploited Children (NCMEC) for identification of known victims. NCMEC reported that at least three (3) video files sent by talentedtongue19@yahoo.com and at least one (1) video file received by talentedtongue19@yahoo.com depicted an identified child victim.

17. Upon further investigation, SA Ruiz identified the account user talentedtongue19@yahoo.com as Randolph G. GUM of Rochester, Pennsylvania. SA Ruiz then forwarded the investigative information to HSI Pittsburgh for further action.

18. In December 2015, your Affiant received the aforementioned investigative lead from SA Ruiz. During your Affiant's review of this information, your Affiant noted several different email accounts associated with Randolph GUM, including talentedtongue19@yahoo.com, talentedtongue14@yahoo.com, talentedtongue14@hotmail.com, and randygum94@gmail.com.

19. While reviewing the information obtained from Yahoo! pursuant to the federal search warrant for the talentedtongue19@yahoo.com account, your Affiant reviewed an email string between talentedtongue19@yahoo.com and damnhegotstupidass@yahoo.com from July 2015. Within this email conversation, talentedtongue19@yahoo.com included an attachment named VID-20140322-WA0007.mp4. Your Affiant reviewed this attachment, which contained a video that is approximately one minute and forty-two seconds in length (1:42) and shows an adult male penis penetrating the anus of a prepubescent male child. Within this same email string, talentedtongue19@yahoo.com writes, "Send me more of what you got" followed by this link to Dropbox:

https://www.dropbox.com/sh/mnrec2g1rwe7lvh/AAD3lC0HtlpcRJw28oc4686oa?dl=0

Your Affiant reviewed this Dropbox link and found that it included approximately 2,479 images, the vast majority of which were child pornography and child erotica depicting prepubescent and pubescent male children.

20. On February 10, 2016, your Affiant served DHS Summons No. ICE-HSI-PB-2016-00067 to Dropbox located at 185 Berry St., Suite 400, San Francisco, CA 94107. The

summons was served via email to legalcompliance@dropbox.com for subscriber information for the aforementioned Dropbox link, as well as for Dropbox user accounts associated with the following email accounts:

talentedtongue19@yahoo.com

talentedtongue14@yahoo.com

talentedtongue14@hotmail.com

randygum94@gmail.com

21. On February 22, 2016, your Affiant received the Dropbox response to DHS Summons No. ICE-HSI-PB-2016-00067. No Dropbox accounts were found for the email addresses talentedtongue19@yahoo.com, talentedtongue14@hotmail.com, or randygum94@gmail.com. For the aforementioned Dropbox link containing images of child pornography, the following account information was found:

Name: randy gum

Email: talentedtongue14@yahoo.com

User: 258796887

Joined: 2014-01-20 01:17:07 GMT

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

22. Based on your Affiant's previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom your Affiant has had discussions, your Affiant has learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual

interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure

and private environment, such as a computer or mobile device. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Those that receive and possess and collect child pornography maintain their collection and material even if they move physical, geographic locations. A collector and user of child pornography who maintains the images and videos in a digital or electronic format, such as on a computer, discs, external hard drive, thumb drives, mobile devices, etc., will take the materials to a new location in the event of a physical move.

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

23. Title 18, United States Code, Chapter 121, Sections 2701 through 2712, is entitled the "Stored Communications Act" (SCA). Section 2703 of the SCA sets forth the procedure that federal and state law enforcement officers follow to compel disclosure of various categories of stored electronic information from service providers. This Court has jurisdiction to issue the

requested warrants because it is "a court of competent jurisdiction" as defined by Section 2711(3)(A)(i) of the SCA. This application is made pursuant to the Stored Communications Act and the Federal Rules of Criminal Procedure.

24. This application seeks a warrant to obtain copies of all files, emails, images, videos, messages, and other information and electronic data that may be found on Dropbox.com servers which pertain to the Dropbox account associated with talentedtongue14@yahoo.com.

CONCLUSION

25. Based upon the information contained in this application and affidavit, there is probable cause to conclude that on the computer systems owned, maintained, and/or operated by Dropbox.com there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) which makes it a crime to receive, distribute or possess material depicting the sexual exploitation of a minor.

26. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

27. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including the Application, Affidavit, and the Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

28. A separate motion for an order requiring non-disclosure of the search warrant to the subscriber pursuant to Title 18, United States Code, Section 2703(b)(1)(A), and Title 18, United States Code, Section 2705(b), is being filed simultaneously herewith.

Respectfully submitted,

MOLLY J. ROCK
Special Agent
Homeland Security Investigations

Subscribed and sworn before me,
This 29th day of February, 2016.

ROBERT C. MITCHELL
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Dropbox account registered to the email address talentedtongue14@yahoo.com, which is stored at premises owned, maintained, controlled, or operated by Dropbox.com, 185 Berry Street, Suite 400, San Francisco, CA 94107.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

I. Information to be Disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox , including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with the file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and email "invites" sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), including for each account listed on Attachment A, information pertaining to the following matters:

a. All images and videos depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256;

b. All electronic communications regarding children engaging in sexually explicit conduct;

c. All communications with potential minors involving sexual topics or in an effort to seduce the minor;

d. Any evidence that would tend to identify the person using the account when any of the items listed in subparagraphs a-c were sent, read, copied or downloaded; or

e. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

III. Method of Delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to Immigration & Customs Enforcement, Homeland Security Investigations, c/o

Special Agent Molly Rock, located at 3000 Sidney Street, Suite 300, in Pittsburgh, Pennsylvania 15203, or Molly.Rock@ice.dhs.gov.